Chapter 1
VPN Overview

A virtual private network (VPN) consists of two topological areas, the provider's network and the customer's network. The provider's network, which runs across the public Internet infrastructure, consists of routers that provide VPN services to a customer's network as well as routers that provide other services. The customer's network is commonly located at multiple physical sites. The provider's network acts to connect the various customer sites in what appears to the customer and the provider to be a private network.

To ensure that VPNs remain private and isolated from other VPNs and from the public Internet, the provider's network maintains policies that keep routing information from different VPNs separate.

A provider can service multiple VPNs as long as its policies keep routes from different VPNs separate. Similarly, a site can belong to multiple VPNs as long as it keeps routes from the different VPNs separate.

VPN Terminology

VPNs contain the following types of network devices (see Figure 1):

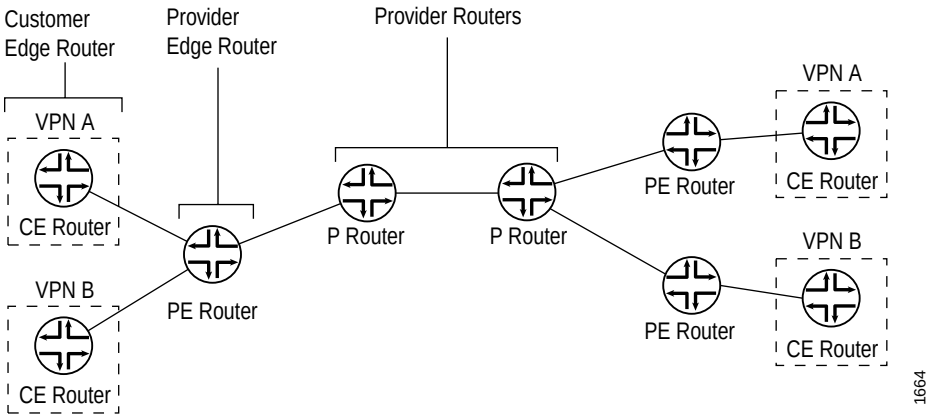
- Provider edge (PE) routers—Routers in the provider's network that connect to customer edge devices located at customer sites. PE routers support VPN and label functionality. (The label functionality can be provided either by the Resource Reservation Protocol [RSVP] or Label Distribution Protocol [LDP].) Within a single VPN, pairs of PE routers are connected through a tunnel, which can be either an Multiprotocol Label Switching (MPLS) label switched path (LSP) or an LDP tunnel.

- Provider (P) routers—Routers within the core of the provider's network that are not connected to any routers at a customer site but are part of the tunnel between pairs of PE routers. Provider routers support MPLS LSP or LDP functionality, but do not need to support VPN functionality.

- Customer edge (CE) devices—Routers or switches located at the customer's site that connect to the provider's network. CE devices are typically IP routers.

VPN functionality is provided by the PE routers; the provider and CE routers have no special configuration requirements for VPNs.

Figure 1: VPN Router Components



Differences between Layer 2 and Layer 3 VPNs

In a Layer 3 VPN, the routing occurs on the service provider's routers. In a Layer 2 VPN, routing occurs on the customer's routers, typically on the CE router. Layer 3 VPNs require more configuration on the part of the service provider, because the service provider's PE routers must know the customer's routes. Layer 2 VPNs require less configuration on the part of the service provider, because routing is handled by the customer's routers and not the service provider's.

VPN Graceful Restart

VPN graceful restart allows a router whose VPN control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts any Layer 2 or Layer 3 VPN services provided by the router.

For VPN graceful restart to function properly, the following needs to be configured on the PE router:

BGP graceful restart must be active on the PE-to-PE sessions carrying any service signaling data in the session's network layer reachability information (NLRI).

OSPF, ISIS, LDP, and RSVP graceful restart must be active, because routes added by these protocols are used to resolve Layer 2 and Layer 3 VPN NLRIs.

For other protocols (static, RIP, OSPF, LDP and so on), graceful restart functionality must also be active when these protocols are run between the PE and CE routers. Layer 2 VPNs do not rely on this because protocols are not configured between the PE and CE routers.

In VPN graceful restart, a restarting router does the following:

Waits for all the BGP NLRI information from other PE routers before it starts advertising routes to its CE routers.

Waits for all protocols in all routing instances to converge (or finish graceful restart) before sending CE router information to the other PE routers.

Waits for all routing instance information (whether it is local configuration or advertisements from a remote peer router) to be processed before sending it to the other PE routers.

Preserves all forwarding state information in the MPLS routing tables until new labels and transit routes are allocated and then advertises them to other PE routers (and CE routers in carrier-of-carriers VPNs).